In re Application of Feldbau et al.
U.S. National Phase of PCT/IB96/00859

C1

recipient, and said one or more information elements a2,...,an comprising dispatch-related information and comprise at least the following elements:

A1 cont

a2 - a time indication associated with said dispatch; and

a3 - information describing the destination of said dispatch,

and wherein at least said information element a2 is provided in a manner that is resistant to or indicative of tampering by either of said sender and said recipient;

means for associating said dispatch-related information with said element a1 by generating authentication-information comprising a representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; and

means for securing at least part of said authentication-information against tampering of at least said sender.

~~65~~ 2. Apparatus according to claim ~~64~~ 1, wherein said element a2 comprises at least one element selected from the group consisting of the date associated with said dispatch, and the time associated with said dispatch.

41

3 ~~66~~. Apparatus according to claim 1 ~~64~~ or 2 ~~65~~, wherein said dispatch-related information comprises at least one element selected from the group consisting of a delivery indication associated with said dispatch, the number of pages transmitted, page numbers, an indication of identification associated with said sender, an indication of identification associated with said recipient, said dispatch duration, integrity information, an indication of dispatch identification associated with said dispatch, an indication of identification associated with said apparatus, a heading message, and a trailing message.

A' cont'd

~~**67.** Apparatus according to claim 64, wherein at least one of the means for associating and for securing comprises means for generating a new set B, said set B comprising one or more information elements b1,...,bm, each element bi comprising a representation of a subset Si, said representation being expressive as a function Fi of the elements of said subset Si, where said subset Si comprises a digital representation of at least one element of said set A, and where said functions Fi can be different.~~

4 ~~68~~. Apparatus according to claim 1 ~~64~~, wherein the elements of said authentication-information have a form selected from the group consisting of the following forms: a

42

In re Application of Feldbau et al.
U.S. National Phase of PCT/IB96/00859

paper document, microfiche and electronic information, and where each of said elements can have different form.

~~69~~ 5. Apparatus according to claim ~~64~~ 1, wherein said element a1 is provided from the sender by electronic means.

E A1 cont

~~70~~ 6. Apparatus according to claim ~~67~~ 64 1, wherein said authentication-information comprises a representation of at least part of said new set B.

~~71~~ 7. Apparatus according to claim ~~69~~ 5, wherein said electronic means comprises a combination of at least one of the following : a communication network, a scanning device, a dispatcher, and a computer.

~~72~~ 8. Apparatus according to claim ~~64~~ 1 or ~~71~~ 7, wherein said dispatcher comprises at least one element selected from the group consisting of a facsimile machine, a modem, a network interface card (NIC), a computer, a communication line, a communication network, an E-Mail system, an EDI system, and a message transmission forwarding service.

~~73~~ 9. Apparatus according to claim ~~64~~ 1, comprising means for authenticating the identity of at least one member selected from the group consisting of said sender, said recipient, an agent of said sender, and an agent of said recipient.

08981461.122597

43

~~74~~ 10. Apparatus according to claim ~~64~~ 1, comprising means for providing said dispatched information to said dispatcher for electronic transmission to said recipient.

Sub C2

A1 cont'd

~~75~~ 11. Apparatus according to claim 64, and comprising at least part of said dispatcher.

~~76~~ 12. Apparatus according to claim ~~64~~ 1, and comprising means for generating selected elements of said set A.

~~77~~ 13. Apparatus according to claim ~~64~~ 1, wherein said element a3 comprises at least one element selected from the group consisting of an address associated with said dispatch, an address associated with said recipient, and an indication of identification associated with said recipient.

~~78~~ 14. Apparatus according to claim ~~66~~ 3, wherein said delivery indication comprises an indication of identification associated with said recipient.

~~79~~ 15. Apparatus according to claim ~~64~~ 1, comprising means for providing an output comprising a representation of at least part of said authentication-information.

~~80~~ 16. Apparatus according to claim ~~64~~ 1, wherein said means for securing comprises secure storage means for storing at least part of said authentication-information.

~~81~~ 17. Apparatus according to claim ~~64~~ ~~67~~ 1, wherein at least one member selected from the group consisting of said function

44

Fi and at least one information element of said new set B, is unknown at least to said sender.

18 ~~82~~. Apparatus according to claim 1, ~~67~~ or 81, wherein said new set B comprises a verifiable digital signature of said subset Si.

19 ~~83~~. Apparatus according to claim 18 ~~82~~, comprising a corresponding verification means for said verifiable digital signature, for authenticating at least one of the following: at least one element of said subset Si, and the originator of said digital signature.

20 ~~84~~. Apparatus according to claim 1 ~~64~~, ~~67~~ or 77, wherein said set A comprises a link information element through which other elements selected from the group consisting of said set A and the authentication-information are linked.

21 ~~85~~. Apparatus according to claim 1 ~~67~~, wherein said function Fi has the property that it is substantially difficult to find a set S' comprising at least one information element, said set S' being different from said subset Si and yet can be used instead, such that applying said function Fi to said set S' will yield said element bi, i.e., such that Fi(S')=bi.

22 ~~86~~. Apparatus according to claim 1 ~~67~~, wherein said function Fi comprises at least one reversible function, comprising means for generating a set C which comprises one or

more information elements c1,...,ck, where said set C is expressive as a function I of at least part of said information element bi, and said function I comprising the inverse function of said reversible function .

87. Apparatus according to claim 64 or 67, comprising means for verifying the authenticity of an information element purported to match a corresponding element of said set A, said verification means comprising means for comparing a representation of said purported information element with a representation of at least part of said authentication-information to determine if they match.

88. Apparatus according to claim 67, comprising means for verifying the authenticity of a set Si' comprising one or more information elements which are purported to match the corresponding elements of said subset Si, said verification means comprising:

means for generating a new information element bi' comprising a representation of said set Si' which is expressive as said function Fi of the elements of said set Si'; and

means for comparing a representation of said element bi' with a representation of said element bi to determine if they match.

46

25 ~~89~~. Apparatus according to claim 1 ~~67~~ 64, wherein said function Fi comprises one or more functions.

26 ~~90~~. Apparatus according to claim ~~82~~ 18, wherein said digital signature is generated according to a scheme selected from the group consisting of secret-key (symmetric) cryptosystems and public-key cryptosystems.

27 ~~91~~. Apparatus according to claim 1 ~~67~~ 64, wherein said new set B comprises an element generated according to a Time Stamping Service scheme.

28 ~~92~~. Apparatus according to claim 1 ~~64 or 67~~, wherein the means for associating is combined with the means for securing.

29 ~~93~~. Apparatus according to claim 1 ~~64~~, wherein said apparatus is associated with a party other than said sender, or is resistant to or indicative of tampering by at least said sender.

Sub C3

30 ~~94~~. A method for authenticating that certain information has been transmitted from a sender via a dispatcher to a recipient, comprising the steps of:

providing a set A comprising a plurality of information elements a1,...,an, where said information element a1 is originated from the sender and comprising the contents of the information being electronically transmitted to said recipient, and said one or more information elements a2,...,an

47

comprising dispatch-related information and comprise at least the following elements:

a2 - a time indication associated with said dispatch; and

C3

a3 - information describing the destination of said dispatch,

and wherein at least said information element a2 is provided in a manner that is resistant to or indicative of tampering by either of said sender and said recipient;

associating said dispatch-related information with said element a1 by generating authentication-information comprising a representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; and

securing at least part of said authentication-information against tampering of at least said sender.

31 ~~95~~. A method according to claim 30 ~~94~~, wherein said dispatch-related information comprises at least one element selected from the group consisting of a delivery indication associated with said dispatch, the number of pages transmitted, page numbers, an indication of identification associated with said sender, an indication of identification associated with said recipient, said dispatch duration,

48

integrity information, an indication of dispatch identification associated with said dispatch, an indication of identification associated with said authenticator, a heading message, and a trailing message.

32 ~~96~~. A method according to claim ~~94~~ 30, comprising the step of authenticating the identity of at least one member selected from the group consisting of said sender, said recipient, an agent of said sender, and an agent of said recipient.

33 ~~97~~. A method according to claim ~~94~~ 30, wherein the elements of said authentication-information have a form selected from the group consisting of the following forms: a paper document, microfiche and electronic information, and where each of said elements can have different form.

34 ~~98~~. A method according to claim ~~94~~ 30, wherein said element a1 is provided from the sender by electronic means.

~~**99.** A method according to claim 94, wherein at least one of the steps of associating and securing comprises the step of generating a new set B, said set B comprising one or more information elements b1,..., bm, each element bi comprising a representation of a subset Si, said representation being expressive as a function Fi of the elements of said subset Si, where said subset Si comprises a digital representation of at least one element of said set A, and where said functions Fi can be different.~~

49

35 ~~100~~. A method according to claim 34 ~~98~~, wherein said electronic means comprises a combination of at least one of the following : a communication network, a scanning device, a dispatcher, and a computer.

34 ~~101~~. A method according to claim 36 ~~94~~ or 35 ~~100~~, wherein said dispatcher comprises at least one element selected from the group consisting of a facsimile machine, a modem, a network interface card (NIC), a computer, a communication line, a communication network, an E-Mail system, an EDI system, and a message transmission forwarding service.

37 ~~102~~. A method according to claim 36 ~~94~~ ~~98~~, wherein said authentication-information comprises a representation of at least part of said new set B.

38 ~~103~~. A method according to claim 36 ~~94~~, comprising the step of providing said dispatched information to said dispatcher for electronic transmission to said recipient.

39 ~~104~~. A method according to claim 36 ~~94~~, wherein said element a2 comprises at least one element selected from the group consisting of the date associated with said dispatch, and the time associated with said dispatch.

40 ~~105~~. A method according to claim 36 ~~94~~, comprising the step of generating selected elements of said set A.

41 ~~106~~. A method according to claim 36 ~~94~~, wherein said element a3 comprises at least one element selected from the group

50

consisting of an address associated with said dispatch, an address associated with said recipient, and an indication of identification associated with said recipient.

42 ~~107~~. A method according to claim ~~95~~ 31, wherein said delivery indication comprises an indication of identification associated with said recipient.

43 ~~108~~. A method according to claim ~~94~~ 30, comprising the step of electronically transmitting said dispatched information to said recipient.

44 ~~109~~. A method according to claim ~~94~~ 36, comprising the step of providing an output comprising a representation of at least part of said authentication-information.

45 ~~110~~. A method according to claim ~~109~~ 44, wherein said step of providing an output provides said output to a party selected from the group consisting of said sender, said recipient, an arbitrator, and a legal authority.

46 ~~111~~. A method according to claim ~~94~~ 36, wherein the step of securing stores at least part of said authentication-information in a secure storage device.

E 47 ~~112~~. A method according to claim ~~99~~ ~~94~~ 36, wherein at least one member selected from the group consisting of said function Fi, and at least one information element of said new set B, is unknown at least to said sender.

51

48 ~~113~~. A method according to claim ~~99~~ ~~94~~ 36 or ~~112~~ 47, wherein said new set B comprises a verifiable digital signature of said subset Si.

49 ~~114~~. A method according to claim ~~113~~ 48, comprising a corresponding verification step for said verifiable digital signature, for authenticating at least one of the following: at least one element of said subset Si, and the originator of said digital signature.

50 ~~115~~. A method according to claim ~~94~~ 30, ~~99~~ or ~~106~~ 41, wherein said set A comprises a link information element through which other elements selected from the group consisting of said set A and the authentication-information are linked.

51 ~~116~~. A method according to claim ~~99~~ ~~94~~ 30, wherein said function Fi has the property that it is substantially difficult to find a set S' comprising at least one information element, said set S' being different from said subset Si and yet can be used instead, such that applying said function Fi to said set S' will yield said element bi, i.e., such that Fi(S')=bi.

52 ~~117~~. A method according to claim ~~99~~ ~~94~~ 30, wherein said function Fi comprises at least one reversible function, comprising the step of generating a set C which comprises one or more information elements c1,...,ck, where said set C is expressive as a function I of at least part of said

52

information element bi, and said function I comprising the inverse function of said reversible function.

~~**118.** A method according to claim 94 or 99, comprising the step of verifying the authenticity of an information element purported to match a corresponding element of said set A, said verification step comprising the step of comparing a representation of said purported information element with a representation of at least part of said authentication-information to determine if they match.~~

A' cont

~~**119.** A method according to claim 99, comprising the step of verifying the authenticity of a set Si' comprising one or more information elements which are purported to match the corresponding elements of said subset Si, said verification step comprising the steps of:~~

Sub E4

~~generating a new information element bi' comprising a representation of said set Si' which is expressive as said function Fi of the elements of said set Si'; and~~

~~comparing a representation of said element bi' with a representation of said element bi to determine if they match.~~

E

55 ~~**120**~~. A method according to claim ~~99~~ ~~94~~ 30, wherein said function Fi comprises one or more functions.

56 ~~**121**~~. A method according to claim ~~113~~ 48, wherein said digital signature is generated according to a scheme selected

53

09981151.122397

from the group consisting of secret-key (symmetric) cryptosystems and public-key cryptosystems.

E

57 ~~122~~. A method according to claim 30 94 ~~99~~, wherein said new set B comprises an element generated according to a Time Stamping Service scheme.

E

58 ~~123~~. A method according to claim 30 ~~94~~ ~~or 99~~, wherein the step of associating is combined with the step of securing.

A1 cont

59 ~~124~~. A method according to claim 30 ~~94~~, wherein the activities described by said steps are being performed by an authenticator, said authenticator being associated with a party other than said sender.

Sub C14

125. A method of authenticating a dispatch and contents of the dispatch transmitted from a sender to a recipient, comprising the steps of:

receiving content data representative of the contents of the dispatch originated from the sender and being electronically transmitted to said recipient, and a destination of the dispatch;

providing an indicia relating to a time of transmission of the dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient;

associating the content data with dispatch record data which includes at least said time related indicia and an

54

C4 cont

indicia relating to the destination of the dispatch, to generate authentication data which authenticate the dispatch and the contents of the dispatch; and

securing at least part of the authentication data against tampering of at least the sender.

A1 cont

61 ~~126~~. A method according to claim ~~125~~ 60, further including the step of transmitting the contents of the dispatch to the recipient.

62 ~~127~~. A method according to claim ~~125~~ 60, further including the step of providing an output of at least part of the authentication data.

~~**128**. A method according to claim 125, wherein at least one of the steps of associating and securing utilizes mathematical association methods for a selected portion of a combination of the content data and the dispatch record data.~~

E

63 ~~129~~. A method according to claim ~~125~~ 60 ~~128~~, wherein the mathematical association methods utilize at least one transform function from a Hiding Class of transform functions.

E

64 ~~130~~. A method according to claim ~~125~~ 60 ~~128~~, wherein the mathematical association methods include a method of generating a digital signature.

65 ~~131~~. A method according to claim ~~125~~ 60, wherein the step of providing the time related indicia includes receiving the time related indicia from an external source.

55

66 ~~132~~. A method according to claim ~~125~~ 60, wherein the step of providing the time related indicia includes generating the time related indicia.

67 ~~133~~. A method according to claim ~~125~~ 60, wherein the step of securing stores at least part of the authentication data in a secure storage device.

E

68 ~~134~~. A method according to claim ~~125 or 128~~ 60, wherein the step of associating is combined with the step of securing.

69 ~~135~~. A method according to claim ~~125~~ 60, wherein the authentication data further includes a delivery indicia relating to said dispatch.

A1 cont

70 ~~136~~. A method according to claim ~~125~~ 60, where the activities described by said steps are being performed by an authenticator, said authenticator being associated with a party other than said sender.

Sub C15

137. An authenticator for authenticating a dispatch and contents of the dispatch transmitted from a transmitting system to a receiving system via an electronic communication network, comprising:

an input unit coupled to the communication network or to the transmitting system for receiving content data representative of the contents of the dispatch being electronically transmitted to said receiving system, and a destination of the dispatch;

56

C15 con't

means for providing an indicia relating to a time of transmission of the dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient;

a processor for associating the content data with dispatch record data which includes at least said time related indicia and an indicia relating to the destination of the dispatch, to generate authentication data which authenticate the dispatch and the contents of the dispatch; and

A1 cont

means for securing at least part of the authentication data against tampering of at least the sender.

72 ~~**138**~~. An authenticator according to claim 71 ~~137~~, further including an output transmitter coupled to the communication network for transmitting the contents of the dispatch to the receiving system.

73 ~~**139**~~. An authenticator according to claim 71 ~~137~~, further including an output device for providing an output of at least part of the authentication data.

74 ~~**140**~~. An authenticator according to claim 71 ~~137~~, wherein the processor is combined with the means for securing.

141. An authenticator according to claim 137 or 140, ~~wherein the processor utilizes mathematical association~~ methods for a selected portion of a combination of the content

57

data and the dispatch ~~record data~~ to generate the ~~authentication~~ data.

75 ~~142~~. An authenticator according to claim ~~141~~ ~~139~~ 71, wherein the mathematical association methods utilize at least one transform function from a Hiding Class of transform functions.

76 ~~143~~. An authenticator according to claim ~~141~~ ~~139~~ 71, wherein the mathematical association methods include a method of generating a digital signature.

77 ~~144~~. An authenticator according to claim ~~137~~ 71, wherein the means for providing the time related indicia receives the time related indicia from an external source.

78 ~~145~~. An authenticator according to claim ~~137~~ 71, wherein the means for providing the time related indicia generates the time related indicia.

79 ~~146~~. An authenticator according to claim ~~137~~ 71, wherein the authentication data further includes a delivery indicia relating to said dispatch.

80 ~~147~~. An authenticator according to claim ~~137~~ 71, including a secure storage device for securing at least part of the authentication data.

81 ~~148~~. An authenticator according to claim ~~137~~ 71, wherein said authenticator is associated with a party other than said sender, or is resistant to or indicative of tampering by at least said sender.

58

Sub C16

149. An information dispatch system in an electronic communication network comprising:

a source transmitting system coupled to the electronic communication network for sending a dispatch;

a destination receiving system coupled to the electronic communication network for receiving the dispatch; and

an authenticator for authenticating the dispatch and contents of the dispatch transmitted from the source transmitting system to the destination receiving system, including:

an input unit coupled to the communication network or to the source transmitting system for receiving content data representative of the contents of the dispatch being electronically transmitted to said destination receiving system, and a destination of the dispatch;

means for providing an indicia relating to a time of transmission of the dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient;

a processor for associating the content data with dispatch record data which includes at least said time related indicia and an indicia relating to the destination of the dispatch, to generate authentication data which authenticate the dispatch and the contents of the dispatch; and

C6 con't

means for securing at least part of the authentication data against tampering of at least the sender.

83 ~~150~~. An information dispatch system according to claim 82 ~~149~~, wherein the authenticator further includes an output device for providing an output of at least part of the authentication data.

A1 cont

~~**151**. An information dispatch system according to claim 149, wherein the processor is combined with the means for securing.~~

08981461 . 122397

E

84 ~~**152**~~. An information dispatch system according to claim 82 ~~149 or 151~~, wherein the processor utilizes mathematical association methods for a selected portion of a combination of the content data and the dispatch record data to generate the authentication data.

85 ~~**153**~~. An information dispatch system according to claim 82 ~~149~~, wherein the means for providing the time related indicia receives the time related indicia from an external source.

86 ~~**154**~~. An information dispatch system according to claim 82 ~~149~~, wherein the means for providing the time related indicia generates the time related indicia.

87 ~~**155**~~. An information dispatch system according to claim 82 ~~149~~, including a secure storage device for securing at least part of the authentication data.

59